ПОЛІПШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ ЗА ДОПОМОГОЮ ЕФЕКТИВНИХ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ (EDMS)

IMPROVEMENT OF INFORMATION SECURITY AT ENTERPRISES WITH THE HELP OF EFFECTIVE ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS (EDMS)

Системи електронного документообігу (EDMS) відіграють важливу роль у забезпеченні інформаційної безпеки підприємства, оскільки дозволяють ефективно управляти документами та інформаційними потоками, знижуючи ризики, пов'язані з втратами або несанкціонованим доступом до даних. Одним із ключових аспектів безпеки є захист конфіденційності, який забезпечується шифруванням даних під час їх передачі та зберігання, а також використанням багатофакторної аутентифікації для доступу до системи. Контроль доступу здійснюється через розмежування прав користувачів, що дозволяє обмежити можливість перегляду, редагування або видалення документів відповідно до ролей співробітників. Крім того, системи забезпечують цілісність документів завдяки механізмам цифрових підписів і веденню журналу змін, що унеможливлює несанкціоноване редагування або знищення документів без фіксації в системі. Важливою перевагою (EDMS) є також підвищення ефективності роботи завдяки автоматизації процесів, але при цьому необхідно особливу увагу приділяти безпеці серверів, захисту від вірусів та зовнішніх атак, щоб уникнути витоків інформації. Інтеграція (EDMS) в інфраструктуру підприємства значно підвищує загальний рівень захисту даних, що сприяє стабільності роботи та забезпеченню довгострокового збереження важливої документації. Отже, організації повинні прийняти найкращі практики для підвищення інформаційної безпеки, що включає впровадження надійних електронних систем управління документами (EDMS). EDMS служать ключовими інструментами для захисту важливої інформації, сприяючи захисту даних за допомогою шифрування, контролю доступу та контрольних журналів. Оскільки підприємства прагнуть посилити свої системи безпеки, розуміння основних функцій EDMS, таких як автентифікація користувачів, відстеження документів і можливості інтеграції з існуючими протоколами безпеки, стає вирішальним.

Ключові слова: *менеджмент, безпековий механізм, аналіз ризиків,системи електронного документообігу.*

Electronic document management (EDMS) systems play an important role in ensuring the security of the enterprise, as they allow efficient management of documents and information flows, reducing the risks associated with loss or unauthorized access to data. By integrating EDMS with enterprise security policies, organizations can greatly enhance the confidentiality, integrity, and availability of their critical documents and data, reducing the risk of breaches and non-compliance. One of the key aspects of security is privacy protection, which is ensured by encrypting data during transmission and storage, as well as using multi-factor authentication to access the system. Access control is carried out through the separation of user rights, which allows you to limit the ability to view, edit or delete documents according to the roles of employees. In addition, systems ensure the integrity of documents thanks to mechanisms of digital signatures and keeping a log of changes, which makes it impossible to edit or destroy documents without authorization in the system. An important advantage of EDMS is also the improvement of work efficiency due to the automation of processes, but at the same time it is necessary to pay special attention to the security of servers, protection against viruses and external attacks in order to avoid information leaks. The integration of EDMS into the infrastructure of the enterprise significantly increases the overall level of data protection, which contributes to the stability of work and ensuring the long-term preservation of important documentation. EDMS serve as key tools for protecting critical information by facilitating data protection through encryption, access control, and audit logs. If an enterprise is looking to strengthen its security system, understanding the basic functions of an EDMS, such as user authentication, document tracking, and the ability to integrate with existing security protocols, becomes true. In addition to the key security features, EDMS also supports scalability, allowing organizations to easily expand their document management capabilities as they grow. This adaptability ensures that the system remains effective even as the volume of documents and users increases. Furthermore, EDMS can be integrated with other enterprise systems such as ERP, CRM, and HRM, creating a unified platform that enhances both security and operational efficiency. Finally, regular updates and maintenance of EDMS ensure that the system remains resilient against evolving cyber threats, keeping the enterprise's data secure over time.

Key words: *management, safety structure, risc analysis, electronic document management (EDMS) systems.*

УДК 658.8
DOI: https://doi.org/10.32782/dees.14-24

Фетісов О.О.[1]
аспірант,
Приватний вищий навчальний заклад
"Європейський університет"

Fetisov Oleksii
Private Higher Education Establishment
"European University"

Постановка проблеми. У сучасному цифровому середовищі, яке швидко розвивається, важливість інформаційної безпеки на підприємствах зросла до безпрецедентного рівня, головним чином через поширення кіберзагроз і все більш витончену тактику, яку використовують зловмисники. Ключові загрози, такі як атаки програм-вимагачів, фішингові схеми та внутрішні загрози, створюють значні ризики не лише для конфіденційних даних, але й для діяльності підприємства в цілому, що часто призводить до фінансових втрат, шкоди репутації та юридичних наслідків.

[1] ORCID: https://orcid.org/0009-0002-7561-5555

Аналіз останніх досліджень і публікацій. Теоретичне обґрунтування та розроблення науково-практичних засад застосування систем електронного документообігу (EDMS) на підприємствах у своїх роботах розглядають українські та зарубіжні автори. Важливий внесок у формування та розвиток питань економічної безпеки зробили такі науковці, як Т. Мачак, О. Дубина, С. Юрченко, А. Жуків, А. Бєляєв та інші. Їхні дослідження значно розширили і поглибили розуміння основних принципів захисту інформації в сучасному цифровому середовищі, що є критично важливим для забезпечення стабільності та конкурентоспроможності підприємств. Зокрема, їхні праці дозволили уточнити підходи до управління інформаційними ризиками за допомогою (EDMS) та розробити ефективні моделі інформаційної безпеки.

Незважаючи на наявні ґрунтовні науково-методологічні дослідження, доцільно зауважити, що потребує подальшого вдосконалення вирішення задач щодо застосування систем електронного документообігу (EDMS) в контексті інформаційної безпеки підприємства.

Постановка завдання. Метою статті є дослідження застосування систем електронного документообігу (EDMS) в контексті інформаційної безпеки підприємств і глибоке вивчення можливостей та викликів, які постають перед організаціями при впровадженні таких систем, з особливим акцентом на забезпеченні інформаційної безпеки. Це дослідження має на меті проаналізувати, як EDMS можуть підвищити ефективність управління документами, знизити ризики втрат або витоків даних, а також посилити контроль над доступом до конфіденційної інформації.

Наукова новизна: полягає у вивченні та впровадженні інноваційних підходів, пов'язаних із застосуванням EDMS у сфері інформаційної безпеки підприємств. Дослідження цієї теми розкриває нові можливості та перспективи, оскільки об'єднує традиційні принципи управління безпекою із передовими технологіями EDMS.

Виклад основного матеріалу дослідження.

Ключові загрози інформаційній безпеці на підприємствах. У сучасному цифровому середовищі підприємства стикаються з безліччю загроз інформаційній безпеці, які вимагають пильного управління та надійних захисних заходів. Однією з головних загроз є несанкціонований доступ до конфіденційної інформації, який серйозно порушує конфіденційність бізнес-операцій і даних [1, с. 42]. Це порушення конфіденційності може призвести до значної репутаційної шкоди та фінансових втрат, підкреслюючи критичну потребу для підприємств у запровадженні суворих систем контролю доступу та моніторингу. Крім того, зростаючий рівень інтелектуалізації та інформатизації в суспільстві підвищує ставки на надійні заходи інформаційної безпеки, оскільки організації тепер повинні захищати більш складну та інтегровану інформаційну екосистему [1, с. 44]. Перетин цих технологічних досягнень із глобальною конкуренцією ще більше посилює ризики, вимагаючи від підприємств не лише захисту своїх даних, але й підтримки конкурентної переваги на інформаційному ринку [1, с. 45]. Для ефективного вирішення цих проблем підприємствам вкрай необхідно інвестувати в комплексні стратегії інформаційної безпеки, які охоплюють як технологічні гарантії, так і політичні заходи, забезпечуючи цілісність, доступність і конфіденційність своїх інформаційних активів.

Інформаційні порушення та їх вплив на діяльність підприємства. Наслідки витоку інформації для операцій підприємства виходять за рамки миттєвої втрати даних, оскільки вони можуть значно погіршити конкурентоспроможність компанії та стабільність роботи. Наприклад, сприйняття вразливості в результаті порушення може підірвати позиції компанії на ринку, оскільки зацікавлені сторони можуть почати розглядати її як менш надійну в обробці конфіденційної інформації [2]. Ця втрата довіри може призвести до зниження лояльності клієнтів і зменшення частки ринку, що, у свою чергу, впливає на прибутковість і потенціал зростання. Крім того, фінансові наслідки порушень є глибокими; підприємства можуть зіткнутися з загрозою банкрутства або вимагати додаткового фінансування для відновлення після наслідків, навіть якщо вони раніше переживали період стабільного розвитку [2]. Ця фінансова напруга ускладнюється потенційними судовими діями, як показано на прикладі випадків, коли порушення призвели до судових позовів і подальшого поглинання знецінених компаній [2]. Такі інциденти підкреслюють необхідність надійних заходів безпеки інформації, подібних до основних функцій безпеки, які захищають від збоїв у роботі в складних сценаріях [2]. Тому підприємства повинні віддавати пріоритет інформаційній безпеці як критичному компоненту своєї операційної стратегії для захисту від далекосяжних наслідків взломів.

Передові практики підвищення інформаційної безпеки. Щоб ефективно підвищити інформаційну безпеку, організації повинні прийняти комплексний підхід, який об’єднує добре встановлені стандарти та практики, такі як ті, що викладені в стандарті ISO/IEC 27001 [3, с. 37]. Ця інтеграція забезпечує ефективний захист систем інформаційної безпеки від нових кіберзагроз і збереження конфіденційності, цілісності та доступності інформації [4, с. 5]. Крім того, для організацій вкрай важливо регулярно оновлювати свої стандарти інформаційної безпеки, щоб відповідати зростаючим вимогам цифрового ландшафту [4, с. 5].

Роблячи це, вони можуть не тільки захистити свої інформаційні активи, але й підвищити довіру до цифрового простору, що має вирішальне значення в сучасному взаємопов'язаному світі [4, с. 5]. Окрім дотримання міжнародних стандартів, організації повинні впроваджувати засоби керування конфігурацією як частину своєї стратегії безпеки. Особливу увагу слід приділити новому елементу керування безпекою A.8.9 – Configuration Management зі стандарту ISO/IEC 27001:2022, який розширює можливості ефективного та безпечного керування конфігураціями системи [4, с. 5]. Застосовуючи ці практики, організації можуть створити надійну структуру інформаційної безпеки, яка не тільки зменшує ризики, але й узгоджується з правовими та нормативними вимогами, забезпечуючи в кінцевому підсумку стійкий захист від потенційних кіберзагроз.

Вплив EDMS на захист даних. Системи електронного документообігу (EDMS) відіграють ключову роль у покращенні захисту даних шляхом підвищення прозорості та ефективності діяльності уряду [5, с. 2]. Оцифровуючи документи та полегшуючи доступ до них, EDMS гарантує, що конфіденційна інформація ретельно керується та захищається від несанкціонованого доступу. Ця прозорість не тільки допомагає підтримувати підзвітність, але й посилює систему безпеки, оскільки цифрові сліди можна відстежувати, щоб запобігти витоку даних. Крім того, EDMS дозволяє безперебійно редагувати історичні документи без необхідності створення нових фізичних копій, тим самим зменшуючи ризик неправильного поводження з документом або його втрату [5, с. 2]. Цей цифровий підхід мінімізує залежність від фізичного зберігання, яке часто є вразливим до пошкодження навколишнього середовища або крадіжки, додатково захищаючи важливу інформацію. Крім того, перехід від паперових систем до електронного управління значно знижує ризик, пов'язаний із втратою паперових документів [5, с. 2]. Цей захист від псування або неправильного розміщення фізичних документів підкреслює ефективність EDMS у збереженні цілісності даних. Підсумовуючи, впровадження EDMS не тільки посилює заходи захисту даних, але й оптимізує державні операції, що вимагає постійних інвестицій і розвитку таких технологій, щоб йти в ногу з проблемами безпеки даних, що розвиваються.

Можливості (EDMS) для захисту інформації. Щоб усунути загрози інформаційній безпеці, особливо в середовищах, де цілісність інформації має першочергове значення, впровадження надійних систем управління електронними документами (EDMS) є надважливою. Однією з основних властивостей (EDMS), яка значно підвищує інформаційну безпеку, є жорсткий контроль прав доступу до документів [6, с. 34]. Ретельно визначаючи привілеї доступу, організації можуть забезпечити захист конфіденційної інформації від несанкціонованого доступу, зберігаючи таким чином цілісність і конфіденційність даних. Крім того, розподіл прав доступу користувачів у відповідності з визначеними посадами або привілеями посилює загальну систему безпеки [6, с. 36]. Це гарантує, що лише уповноважений персонал може отримати доступ до певних документів, що має вирішальне значення для захисту інформації підприємства. Крім того, використання обов'язкового доступу та міток безпеки додатково розширює механізм захисту інформації в EDMS [6, с. 37]. Такі мітки забезпечують додатковий рівень безпеки, класифікуючи документи на основі їхнього рівня конфіденційності, таким чином сприяючи кращому контролю над їх розповсюдженням і доступом. Разом ці функції не тільки підвищують рівень безпеки організації, але й забезпечують дотримання правових і нормативних стандартів, що в кінцевому підсумку зменшує ризики, пов'язані з витоком інформації та несанкціонованим доступом. Оскільки підприємства орієнтуються на глобальний інформаційний ринок, впровадження комплексної EDMS із цими функціями безпеки є життєво важливим для підтримки конкурентної переваги та захисту конфіденційних даних.

Інтеграція EDMS в існуючі протоколи безпеки. Інтеграція електронної системи управління документами (EDMS) в існуючі протоколи безпеки вимагає комплексного підходу, який охоплює як технологічні, так і процедурні аспекти. Оскільки системи EDMS часто працюють на розподілених архітектурах, вони вимагають використання різноманітних технологій для забезпечення надійної безпеки [7, с. 34]. Боротьба з потенційними загрозами безпеці включає роздвоєний фокус як на мережевих, так і на локальних атаках, які зазвичай поширюються шкідливими програмами, такими як трояни та руткіти [8, с. 39]. Щоб ефективно пом'якшити ці загрози, організація повинна провести ретельну оцінку безпеки та впровадити захисні заходи, адаптовані до конкретних вразливостей, виявлених у її інформаційному середовищі [8, с. 42]. Використовуючи доступну документацію та практичні поради в таких сферах, як безпека даних і конфігурація системи, підприємства можуть посилити свої заходи безпеки та гарантувати, що їх EDMS бездоганно включено в існуючу систему безпеки [9, с. 16]. Ця стратегічна інтеграція не тільки зміцнює захист організації від можливих порушень, але й оптимізує операції, тим самим зберігаючи цілісність і безперервність бізнес-процесів у все більш цифровому середовищі.

Провідні технології EDMS доступні сьогодні. На сьогоднішній стан технологій EDMS значною мірою впливає ряд систем, які задовольняють різноманітні потреби підприємств. Системи

вітчизняного виробництва набули популярності завдяки їх адаптованості до місцевих вимог і економічній ефективності, а **Мегаполіс** став найпопулярнішим вибором серед вітчизняних підприємств [10, с. 58]. Ця перевага значною мірою зумовлена фінансовими обмеженнями, з якими стикаються ці підприємств, і потребою в рішеннях, які відповідають реаліям їхньої діяльності [10, с. 58]. Примітно, що колись панували системи російського походження, такі як **BOSS-Referent, CompanyMedia** та інші, поточний геополітичний клімат і погіршення дипломатичних відносин зробили їх використання менш актуальним [10, с. 58]. Натомість помітний зсув у бік впровадження українських систем, таких як **Атлас ДОК**, **Мегаполіс** та **Документообіг**, які все частіше отримують визнання за свою ефективність та відповідність внутрішнім потребам [10, с. 58]. Цей перехід підкреслює ширшу тенденцію в секторі, де наголос робиться на використанні місцевих технологій, які пропонують баланс продуктивності та доступності, гарантуючи, що підприємств можуть задовольняти свої потреби в управлінні документами, не несучи надмірних витрат.

EDMS та питання безпеки. Сучасні технології EDMS використовують багатогранний підхід до вирішення проблем безпеки, приділяючи значну увагу управлінню доступом і захисту документів. Розподіляючи права доступу користувачів на основі посади або привілеїв, EDMS може ефективно покращити систему безпеки, гарантуючи, що особи отримають доступ лише до інформації, необхідної для їхніх ролей [11, с. 12]. Цей підхід доповнюється використанням мандатного доступу та міток безпеки, які підсилюють механізми захисту інформації, надаючи додатковий рівень безпеки, який пом'якшує різні загрози [11, с. 12]. Крім того, інтеграція технологій EDMS із специфічними для підприємства завданнями та вимогами дозволяє індивідуально реагувати на проблеми безпеки, що має вирішальне значення для підтримки безпечного середовища, адаптованого до унікальних викликів кожної організації [11, с. 12]. Оскільки підприємства продовжують рости та працювати в територіально розподілених середовищах, здатність EDMS підтримувати таке розширення, одночасно вирішуючи проблеми безпеки, стає все більш важливою [11, с. 12]. Ця всеохоплююча стратегія безпеки не лише бореться з безпосередніми загрозами, але й дає можливість підприємствам ефективно керувати майбутніми ризиками, посилюючи потребу в постійній оцінці та адаптації технологій EDMS до мінливих ландшафтів безпеки.

Обмеження існуючих EDMS у забезпеченні безпеки. Обмеження існуючих систем управління електронними документами (EDMS) у забезпеченні безпеки є багатогранними, причому технології штучного інтелекту відіграють вирішальну роль як у потенційних рішеннях, так і в невід'ємних проблемах. Однією з важливих проблем є непрозорість більшості алгоритмів ШІ, що обмежує прозорість і розуміння, необхідні для надійних заходів безпеки [12, с. 78]. Цей брак прозорості може перешкоджати здатності виявляти загрози безпеці та ефективно реагувати на них, оскільки користувачі чи розробники часто не повністю розуміють внутрішню роботу систем ШІ. Крім того, трудомісткий характер процедур моделювання та калібрування системи створює додаткову проблему, оскільки ці процеси можуть затримувати впровадження необхідних оновлень безпеки та адаптацій, роблячи системи вразливими до нових загроз [12, с. 80]. Ці проблеми ускладнюються неадекватністю поточної законодавчої бази, яка може не повністю підтримувати інтеграцію технологій штучного інтелекту в EDMS, таким чином перешкоджаючи їх потенціалу посилення заходів безпеки [12, с. 83]. Цей законодавчий недолік може призвести до невизначеності та небажання приймати передові рішення штучного інтелекту, оскільки організації можуть побоюватися невідповідності або непередбачуваних правових наслідків. Щоб усунути ці обмеження, організаціям вкрай необхідно наполягати на більш прозорих моделях штучного інтелекту, оптимізувати процеси калібрування та виступати за правову базу, яка підтримує безпечну інтеграцію передових технологій.

Алгоритм успішного впровадження EDMS. Успішне впровадження Системи електронного документообігу (EDMS) передбачає низку методичних кроків, які забезпечують плавний перехід та інтеграцію в існуючі робочі процеси. Початковий крок передбачає всебічну оцінку поточних процесів управління документами в організації для виявлення неефективності та областей для покращення. Ця оцінка повинна включати взаємодію із зацікавленими сторонами для збору їх внеску та розуміння конкретних вимог різних відділів. Після цього необхідно розробити чіткий план із зазначенням цілей, обсягу та очікуваних результатів впровадження EDMS. Цей план має включати навчальні заняття для персоналу з нової системи, щоб вони зрозуміли її функції та могли ефективно її використовувати. Крім того, вкрай важливо вибрати EDMS, яка відповідає цілям організації та пропонує масштабованість для майбутнього зростання. Необхідно уважно стежити за процесом впровадження з регулярними циклами зворотного зв'язку для оперативного вирішення будь-яких проблем. Дотримуючись цих кроків, організації можуть досягти успішного впровадження EDMS, що призведе до підвищення ефективності, зниження витрат і покращення доступності та безпеки документів.

Налаштування EDMS для конкретних потреб безпеки підприємства. Щоб вирішити проблеми з безпекою, підприємства повинні налаштувати свої системи керування електронними документами (EDMS) відповідно до своїх конкретних потреб, тим самим підвищуючи загальну безпеку інформації. Ця настройка передбачає інтеграцію EDMS з іншими заходами корпоративної інформаційної безпеки, забезпечуючи комплексний підхід, який захищає конфіденційну інформацію від потенційних порушень [13, с. 39]. Процес інтеграції вимагає глибокого розуміння унікальних вимог до безпеки організації, які можуть значно відрізнятися залежно від характеру бізнесу та типів документів, що обробляються [14, с. 47]. Крім того, налаштування EDMS також має включати створення та налаштування процедур обробки електронних документів. Це коригування необхідне для врахування будь-яких змін, які можуть виникнути внаслідок розвитку загроз безпеці, таким чином гарантуючи, що EDMS залишається надійною та стійкою [15, с. 43]. Пристосовуючи ці системи до своїх конкретних потреб у безпеці, підприємства можуть пом'якшити ризики, пов'язані з цілісністю, доступністю та конфіденційністю їх інформації, тим самим позиціонуючи себе більш конкурентоспроможними на глобальному інформаційному ринку.

Проблеми під час впровадження EDMS. Підприємства, які починають впровадження системи електронного документообігу (EDMS), стикаються зі значними проблемами, особливо у сфері інформаційної безпеки. Найголовнішим серед них є необхідність забезпечити надійні заходи безпеки, які захищають конфіденційні дані від злому на етапі переходу. Оскільки компанії все більше покладаються на цифрові інструменти для управління своїми операціями, ризик несанкціонованого доступу або витоку даних зростає, створюючи загрозу не лише для внутрішніх процесів підприємства, але й для його репутації та дотримання нормативних стандартів. Ця цифрова залежність підкреслює важливість інтеграції комплексних протоколів безпеки, які відповідають існуючій IT-інфраструктурі для захисту від вразливостей. Крім того, перехід на СЕД може спричинити опір співробітників, які звикли до традиційної практики документообігу. Подолання цього опору вимагає не лише технічних рішень, але й стратегічних зусиль щодо управління змінами, щоб забезпечити плавний процес впровадження. Вирішення цих проблем передбачає багатогранний підхід, який поєднує технічні вдосконалення з ініціативами щодо організаційних змін, забезпечуючи таким чином як безпеку, так і прийняття нової системи. Отже, організації повинні визначити пріоритетність планування та навчання, щоб зменшити ризики та сприяти успішному впровадженню EDMS.

Висновки. У сучасному цифровому середовищі потреба в надійній інформаційній безпеці на підприємствах є більш помітною, ніж будь-коли, особливо в світлі багатогранних загроз, які створює несанкціонований доступ до конфіденційної інформації. Це дослідження підкреслює важливу роль, яку відіграють системи керування електронними документами (EDMS) у підвищенні загальної безпеки організацій. Завдяки інтеграції суворого контролю доступу та протоколів моніторингу EDMS не лише захищає критично важливу інформацію, але й відповідає міжнародним стандартам відповідності, забезпечуючи таким чином цілісність, конфіденційність і доступність активів даних. Висновки показують, що фінансові наслідки витоку інформації виходять далеко за межі негайної втрати даних, охоплюючи репутаційну шкоду та потенційне банкрутство, що вимагає проактивного підходу до прийняття комплексних стратегій інформаційної безпеки. Крім того, успішне впровадження EDMS залежить від ретельного процесу налаштування, адаптованого до конкретних операційних потреб організації, таким чином пом'якшуючи ризики, пов'язані з моральним старінням і неефективною інтеграцією системи. Незважаючи на те, що дослідження підкреслює переваги переходу від традиційних паперових систем до електронного управління, воно також визнає проблеми, властиві таким перетворенням, включаючи необхідність постійного оновлення протоколів безпеки та конфігурацій доступу користувачів. Примітно, що включення найкращих практик, таких як ті, що описані в ISO/IEC 27001, служить основоположним елементом для створення стійкої структури інформаційної безпеки. Однак важливо визнати потенційні обмеження в дослідженні, такі як різний ступінь впровадження технологій у різних секторах, які можуть вплинути на застосовність результатів. Майбутні дослідження мають вивчити мінливий ландшафт кіберзагроз і ефективність нових технологій у зміцненні функцій безпеки EDMS, особливо в умовах, коли організації стикаються зі зростаючим тиском глобальної конкуренції та нормативних вимог. Зрештою, ця дискусія ще раз підтверджує необхідність для підприємств віддавати пріоритет інформаційній безпеці як життєво важливому компоненту своїх операційних стратегій, гарантуючи, що вони залишатимуться стійкими до потенційних порушень, зберігаючи при цьому конкурентну перевагу на глобальному інформаційному ринку.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Сороківська О.О., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*, 2017. № 2. Т. 2 С. 42–45.

2. Іванова В.В. Інформаційна безпека як підсистема в системі економічної безпеки підприємства. URL: https://eprints.kname.edu.ua/38599/1/67-71.pdf (дата звернення: 17.10.2024).

3. Yakymenko Y., Muzhanova T., Lehominova S. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії Fireeye. *Кібербезпека: освіта, наука, техніка.* 2021. Вип. 4(12) 2021. С. 36–50. DOI: https://doi.org/10.28925/2663-4023.2021.12.3650 (дата звернення: 19.10.2024).

4. Курій Є. О., Опірський І. Р., Використання шаблонів cis бенчмарк для виконання вимог міжнародного стандарту ISO/IEC 27001:2022 *-(91-100)*. Computer systems and networks vol. 6, no. 1, 2024. DOI: https://doi.org/10.23939/csn2024.01.089 (дата звернення: 20.10.2024).

5. Барегамян С.Х., Карпі Ю.В. Електронне урядування на загальнодержавному, регіональному та місцевому рівнях: сучасний стан та перспективи впровадження в Україні. *Державне управління: удосконалення та розвиток*. 2019. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1522 DOI: https://doi.org/10.32702/2307-2156-2019.11.30 (дата звернення: 24.10.2024).

6. Гарасим О.М. Аналіз засобів управління корпоративною конфіденційною інформацією. *Вісник національного університету "Львівська політехніка".* 2019. № 3. С 34–37.

7. Наукова розробка "Застосування новітніх комп'ютерних технологій. URL: https://naurok.com.ua/test/vidi-suchasnih-komp-yuteriv-ta-h-zastosuvannya-1124146.html.ua (дата звернення: 23.10.24)

8. Програмування та захист інформації, електронний ресурс : зб. Наук. Ст. Студ. / відп. Ред. Т. О. Жирова. Київ : держ. Торг.-екон. Ун-т, 2024. Ч. 2. С. 180.

9. Задорожна Н.Т., Лавріщева К.М. Менеджмент документообігу в інформаційних системах освіти (для ВНЗ і ППО). Навчально-методичний посібник. Київ: КП Видавництво «Педагогічна думка». 2023. С. 1–220. ISBN 978-966-644-052-8

10. Каплун В.В. Інформаційні технології в архівній справі: особливості та проблеми впровадження. *Збірник наукових статей. Інститут економіки, управління та інформаційних технологій*, 2019. С. 58–63.

11. Острівний Д.А. Методи та моделі забезпечення безпеки інформації в системах електронного документообігу комерційного підприємства. URL: https://ir.nmu.org.ua/bitstream/handle/123456789/154433.pdf (дата звернення: 18.10.24.)

12. Машталяр О.М. Проблеми використання штучного інтелекту під час оброблення персональних даних та напрями їх вирішення. *Юридичний науковий електронний журнал*. 2024. № 8. С. 78–83.

13. Василюк А. П. Вдосконалення роботи фахівців охорони праці за рахунок впровадження систем електронного документообігу : Цивільна безпека. Хмельницицький: Нац. Ун-т. Хмельницький, 2022. 63 с.

14. Чумадевська, Х. В. Метод кластеризації набору документів для ведення електронного документообігу. Тернопіль : ЗУНУ, 2023. 80 с.

15. Новікова Д.О. Специфіка роботи з документами обмеженого доступу (на прикладі діяльності військової частини). Полтава : Національний університет "Полтавська політехніка імені Юрія Кондратюка", 2024. 59 с.

REFERENCES:

1. Sorokivska O.O., Hevko V.L. (2017) Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy [Enterprise information security: new threats and prospects]. *Visnyk Khmelnytskoho natsionalnoho universytetu*, no. 2, vol. 2, pp. 42–45.

2. Ivanova V.V. Informatsiina bezpeka yak pidsystema v systemi ekonomichnoi bezpeky pidpryiemstva [Information security as a subsystem in the economic security system of the enterprise]. Available at: https://eprints.kname.edu.ua/38599/1/67-71.pdf

3. Yakymenko Y., Muzhanova T., Lehominova S. (2021). Systemnyi analiz tekhnichnykh system zabezpechennia informatsiinoi bezpeky pidpryiemstv vid kompanii Fireeye [System analysis of technical systems for ensuring information security of enterprises from the Fireeye company]. *Kiberbezpeka: osvita, nauka, tekhnika*, no. 4(12), pp. 36–50. DOI: https://doi.org/10.28925/2663-4023.2021.12.3650 (accessed Octomber 19, 2024).

4. Kurii Ye. O., Opirskyi I. R. (2024) Vykorystannia shabloniv cis benchmark dlia vykonannia vymoh mizhnarodnoho standartu ISO/IEC 27001:2022-(91-100) [Use of cis benchmark templates to meet the requirements of the international standard ISO/IEC 27001:2022 -(91-100)]. *Computer systems and networks*, vol. 6, no. 1. DOI: https://doi.org/10.23939/csn2024.01.089 (accessed Octomber 20, 2024).

5. Barehamian C.Kh., Karpi Yu.V. (2019) Elektronne uriaduvannia na zahalnoderzhavnomu, rehionalnomu ta mistsevomu rivniakh: suchasnyi stan ta perspektyvy vprovadzhennia v Ukraini [Electronic governance at the national, regional and local levels: current state and prospects of implementation in Ukraine]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, no. 11. Available at: http://www.dy.nayka.com.ua/?op=1&z=1522 DOI: https://doi.org/10.32702/2307-2156-2019.11.30 (accessed Octomber 24, 2024).

6. Harasym O.M. (2019) Analiz zasobiv upravlinnia korporatyvnoiu konfidentsiinoiu informatsiieiu [Analysis of corporate confidential information management tools]. *Visnyk natsionalnoho universytetu "Lvivska politekhnika",* no. 3, pp. 34–37.

7. Naukova rozrobka "Zastosuvannia novitnikh kompiuternykh tekhnolohii [Scientific development "Application of the latest computer technologies]. Available at: https://naurok.com.ua/test/vidi-suchasnih-komp-yuteriv-ta-h-zastosuvannya-1124146.html ua (accessed Octomber 23, 2024)

8. Zhyrova T.O. (2024) Prohramuvannia ta zakhyst informatsii [Programming and information protection, electronic resource]. Kyiv : Derzh. Torh.-ekon. Un-t, 180 p.

9. Zadorozhna N.T., Lavrishcheva K.M. (2023) Menedzhment dokumentoobihu v informatsiinykh systemakh osvity (dlia VNZ i PPO). Navchalno-metodychnyi

posibnyk [Management of document flow in education information systems (for universities and vocational training). Educational and methodological guide]. Kyiv: KP Vydavnytstvo «Pedahohichna dumka», 220 p.

10. Kaplun V.V. (2019) Informatsiini tekhnolohii v arkhivnii spravi: osoblyvosti ta problemy vprovadzhennia. *Zbirnyk naukovykh statei. Instytut ekonomiky, upravlinnia ta informatsiinykh tekhnolohii*, pp. 58–63.

11. Ostrivnyi D.A. Metody ta modeli zabezpechennia bezpeky informatsii v systemakh elektronnoho dokumentoobihu komertsiinoho pidpryiemstva [Methods and models of ensuring information security in electronic document flow systems of a commercial enterprise]. Available at: https://ir.nmu.org.ua/bitstream/handle/123456789/154433.pdf (accessed October 18, 2024)

12. Mashtaliar O.M. (2024) Problemy vykorystannia shtuchnoho intelektu pid chas obroblennia personalnykh danykh ta napriamy yikh vyrishennia [Problems of using artificial intelligence during processing of personal data and ways to solve them]. *Yurydychnyi naukovyi elektronnyi zhurnal*, no. 8, pp. 78–83.

13. Vasyliuk A. P. (2023) Vdoskonalennia roboty fakhivtsiv okhorony pratsi za rakhunok vprovadzhennia system elektronnoho dokumentoobihu : Tsyvilna bezpeka [Improving the work of labor protection specialists due to the introduction of electronic document management systems: Civil safety]. Khmelnytsytskyi: Nats. Un-t. Khmelnytskyi, 63 p.

14. Chumadevska Kh. V. (2023) Metod klasteryzatsii naboru dokumentiv dlia vedennia elektronnoho dokumentoobihu [The method of clustering a set of documents for electronic document management]. Ternopil : ZUNU, 80 p.

15. Novikova D.O. (2024) Spetsyfika roboty z dokumentamy obmezhenoho dostupu (na prykladi diialnosti viiskovoi chastyny) [The specifics of working with restricted access documents (on the example of the activities of a military unit)]. Poltava : Nats. Un-t im. Yuriia Kondratiuka, 59 p.